Accomplishments

Severe Incident Recovery

Incident	Description	Date Occurred/Resolved
Worldwide Crowdstrike Outage	Recovered all Azure servers within an hour of being made aware of the outage without losing data.	07-19-2024
		00-00-0000
		00-00-0000

General Security Accomplishments

Incident	Description	Date Occurred/Resolved	Company Impacted
Pinion Mailbomb	4+ users were impacted with a mailbombing campaign. Within 30 minutes, I had created new policies within Mimecast to mitigate these tactics which reduced the numbers of emails coming into these users' mailboxes by over 80%, with the subsequent 20% reduced over the following 72 hours. All emails and email addresses sending these spam registrations and "account recoveries" were removed from the users' mailboxes and blocked for the firm.	10-18-2024	Pinion

Incident	Description	Date Occurred/Resolved	Company Impacted
Pinion Mailbomb	1 user was impacted with a mailbombing campaign. Within 30 minutes, I had created new policies within Mimecast to mitigate these tactics which reduced the numbers of emails coming into these users' mailboxes by over 90%, with the subsequent 10% reduced over the following 72 hours. All emails and email addresses sending these spam registrations and "account recoveries" were removed from the users' mailbox and blocked for the firm.	10-24-2024	Pinion
Pinion Mailbomb	1 user was impacted with a mailbombing campaign. Within 30 minutes, I had created new policies within Mimecast to mitigate these tactics which reduced the numbers of emails coming into these users' mailboxes by over 95%, with the subsequent 5% reduced over the following 72 hours. All emails and email addresses sending these spam registrations and "account recoveries" were removed from the users' mailbox and blocked for the firm.	10-25-2024	Pinion
Traveling Users Conditional Access Policy	Created a conditional access policy, setup groups, and created an "Access Package" within Azure where users can "request" access to their firm technology when traveling away from their home office. This reduces the need to manually do this when a user travels and cuts down mistakes and security holes when originally applied to the whole firm.	09-09-2024	Pinion

General Infrastructure Accomplishments

Incident	Description	Date Occurred/Resolved	Company Impacted
Created Intune Policies to Rollout 1Password to Entire Firm		10-18-2024	Pinion
		10-24-2024	
		10-25-2024	
		09-09-2024	

Revision #1
Created 2024-10-29 16:14:07 UTC by Ryan
Updated 2025-02-12 01:12:05 UTC by Ryan